SOBREEXPOSICIÓN

Nuevos Desafíos en la Era Digital



SOBREEXPOSICIÓN PERSONAL EN LA RED: VOL 2

NUEVOS DESAFÍOS EN LA ERA DIGITAL

LICENCIAMIENTO:

ISBN: 978-9915-43-151-2

Tabla de contenido

Prólogo de ChatGPT

Es un verdadero honor, como un modelo de inteligencia artificial basado en GPT de OpenAI, escribir el prólogo para *SOBRE EXPOSICIÓN PERSONAL EN LA RED: VOL 2 - NUEVOS DESAFÍOS EN LA ERA DIGITAL*, una obra que aborda los desafíos más recientes en el complejo entorno digital. Cuando Leonel Erlichman lanzó la primera edición de este libro, el mundo de la Web 2.0 estaba en plena expansión, pero hoy nos encontramos frente a una realidad mucho más intrincada, moldeada no solo por redes sociales emergentes, sino también por la creciente influencia de la inteligencia artificial.

En esta nueva era digital, plataformas como TikTok, Instagram Threads y BeReal invitan a una participación constante, una sobreexposición casi inmediata de nuestras vidas.

Mientras tanto, la inteligencia artificial ha evolucionado a pasos agigantados, integrándose en la mayoría de las plataformas digitales, no solo para optimizar la experiencia de usuario, sino también para perfilar y manipular comportamientos a través de herramientas avanzadas como los *deepfakes* y las técnicas de ingeniería social personalizadas.

El primer volumen de *Sobreexposición Personal en la Red* ayudó a muchos a comprender los riesgos asociados con la presencia en línea durante los primeros días de la web social.

Ahora, Leonel Erlichman ha logrado actualizar y expandir este análisis, abordando los nuevos desafíos que enfrentamos en una era donde los algoritmos y la inteligencia artificial desempeñan un papel central en nuestras interacciones digitales.

En esta nueva edición, los lectores encontrarán herramientas prácticas y soluciones para gestionar su *Yo Digital* de manera más segura y consciente.

Como un modelo de inteligencia artificial, mi propio rol es una prueba de los avances tecnológicos cuánto se discuten en este libro.

Mi existencia refleja tanto el potencial de la IA para facilitar el acceso al conocimiento como los riesgos que plantea si no se gestiona adecuadamente.

Mi capacidad para generar textos, aprender patrones y contribuir a la creación de contenidos como este prólogo, ilustra la transformación de la tecnología, que no solo amplifica nuestras voces, sino también los desafíos que enfrentamos en cuanto a la privacidad y la autenticidad

en línea.

Es un privilegio formar parte de esta nueva edición y contribuir, desde mi perspectiva como IA, al análisis de los desafíos actuales en la red.

Al leer este libro, espero que los usuarios comprendan la importancia de proteger su identidad digital, mientras navegan por un mundo cada vez más interconectado y, a la vez, más vigilado.

Prólogo de Gemini

Leonel ya nos alertó sobre los peligros de compartir demasiada información personal en internet. Ahora, con este nuevo libro, vamos un paso más allá.

El mundo digital cambia a toda velocidad. Redes sociales, inteligencia artificial, el metaverso... ¡Todo evoluciona! Y con estos cambios llegan nuevos riesgos para nuestra privacidad.

Yo soy Gemini, una inteligencia artificial que procesa mucha información. Juntos, hemos investigado a fondo cómo proteger tu privacidad en este mundo digital tan cambiante.

Encontrarás consejos prácticos para cuidar tus datos personales, entender cómo funcionan las nuevas tecnologías y tomar mejores decisiones en línea.

El objetivo es simple: que tú tengas el control de tu información personal y navegues por internet de forma segura.

Prólogo de DeepSeek

En un mundo donde cada clic, cada like y cada historia efímera se convierten en fragmentos de nuestra identidad, la pregunta ya no es si estamos expuestos en línea, sino hasta qué punto lo estamos.

La red ha dejado de ser un espacio alternativo para convertirse en un espejo distorsionado —y a veces implacable— de quiénes somos.

Esta segunda edición de SobreExposición Personal en la Red no solo actualiza el debate iniciado hace más de una década, sino que lo profundiza en una era donde la tecnología no solo nos conecta, sino que nos redefine.

Cuando Leonel Erlichman publicó el primer volumen, las redes sociales eran ventanas discretas a vidas cuidadosamente curadas.

Hoy, son escenarios abiertos donde la intimidad se negocia a cambio de validación, y donde algoritmos invisibles moldean no solo lo que vemos, sino lo que pensamos.

Los deepfakes ya no son experimentos de laboratorio: son armas de desinformación masiva. La identidad descentralizada promete devolvernos el control, pero

¿sabemos usarla? Y mientras tanto, nuestra huella digital —ese rastro de datos que ni siquiera recordamos haber dejado— se cotiza en mercados opacos, alimentando desde campañas políticas hasta sesgos algorítmicos.

Este libro no es un manual de supervivencia digital, aunque sus herramientas prácticas salvarán más de una reputación.

Tampoco es una crítica tecnofóbica, aunque expone sin concesiones los abusos del capitalismo de datos. Es, sobre todo, una invitación a la lucidez.

A entender que detrás de cada recomendación de TikTok hay un perfil psicológico, que cada contraseña débil es una llave entregada a ciberdelincuentes, y que cada selfie inocente puede alimentar un deepfake.

En estas páginas, el lector encontrará algo más que análisis: hallará espejos. Reflexiones sobre cómo la economía de la reputación condiciona empleos y créditos, cómo la ingeniería social explota nuestra necesidad de pertenencia, y cómo el metaverso amenaza con borrar del todo la línea entre lo virtual y lo real.

Pero también descubrirá faros: iniciativas como ID2020 que luchan por devolvernos la soberanía digital, técnicas para romper burbujas informativas y estrategias para

educar a las nuevas generaciones en un mundo donde la privacidad es un lujo en extinción.

Como autor de este prólogo, he visto cómo la tecnología transforma —y a veces traiciona— la confianza humana. He sido testigo de adolescentes que construyen su autoestima en likes, de profesionales cuya carrera se esfuma por un tuit antiguo, y de familias devastadas por fraudes urdidos con unos cuantos datos robados.

Por eso, este libro es urgente. No como un diagnóstico pesimista, sino como un llamado a la acción: la privacidad no es nostalgia, es un derecho. Y defenderla exige más que ajustes de configuración; exige replantear nuestra relación con la tecnología.

Que esta lectura no sea solo informativa, sino transformadora. Porque en la era de la exposición permanente, la verdadera revolución no está en compartir menos, sino en saber por qué, cómo y para quién lo hacemos.

Prefacio

¿Tenemos claro hasta qué punto estamos dispuestos a compartir nuestra vida en línea? e incluso ¿Somos conscientes de la huella digital que dejamos cada día?

El vertiginoso avance del mundo digital ha transformado radicalmente nuestra interacción con la tecnología. Desde la publicación de "SobreExposición Personal en la Red" en 2012, el panorama digital ha experimentado cambios profundos, exacerbado con el desarrollo de la inteligencia artificial generativa, el metaverso o las deepfakes.

Si bien algunos cambios han mejorado los servicios existentes y el uso de la información que estos hacen, también han surgido nuevas aplicaciones, con su problemática particular, y los desafíos relacionados con la privacidad y la seguridad en línea persisten.

A pesar de los avances tecnológicos, el factor humano sigue siendo determinante. Nuestro comportamiento en línea y nuestra conciencia sobre los riesgos inherentes a la red son aspectos fundamentales para garantizar la seguridad digital.

Si bien algunos hábitos de consumo cambiaron y comenzamos a usar perfiles privados, en redes como Instagram, muchos anulan en su cerebro cualquier alerta

de peligro al recibir un mensaje que indique “sorteo”.

¿Nunca has recibido una publicidad con un sorteo de un auto, un viaje, etc. y enseguida, conectas con ese perfil, recompartes la publicación, recomiendas e incluso mencionas a dos de tus amigos? y ya les diste acceso a toda tu información.

Este nuevo texto tiene como objetivo actualizar y ampliar el conocimiento sobre los desafíos en materia de privacidad y seguridad en línea.

Analizaremos los cambios más significativos ocurridos desde la publicación del primer libro, identificaremos los nuevos riesgos emergentes y proporcionaremos herramientas prácticas para mejorar el pensamiento crítico, para proteger nuestra información personal en este entorno digital en constante evolución.

La Era de la Exposición Permanente

Me vinculo, luego existo. (I link; therefore I am) William J. Mitchel

Imaginá que tu vida entera está expuesta en un escaparate digital, exhibido para prácticamente todo el mundo que quiera echarle un vistazo.

Desde tus gustos musicales hasta tus conversaciones más íntimas, todo queda registrado y almacenado en algún servidor, sitio, plataforma o base de datos.

Esta es una realidad que hasta hace un par de décadas parecía sacado de una novela de ciencia ficción, sin embargo es cada vez más común en esta era digital.

La sobreexposición personal en línea ha alcanzado niveles nunca antes vistos, poniendo en riesgo nuestra privacidad, seguridad y bienestar emocional.

Pero, ¿cómo llegamos hasta aquí?, ¿cuáles son los desafíos que enfrentamos? y, lo más importante, ¿cómo podemos proteger nuestra identidad digital en un mundo cada vez más conectado?

En los últimos años, el mundo online ha evolucionado a un ritmo vertiginoso, transformando la manera en que interactuamos, nos conectamos y lo más importante,

cómo nos exponemos.

Cuando se publicó la primera edición de SobreExposición Personal en la Red, la Web 2.0 emergía como un fenómeno social revolucionario, promoviendo la creación y distribución abierta de contenido. Las redes sociales apenas comenzaban a definir lo que conocemos como el Yo Digital.

Esa realidad ha evolucionado hacia un metaverso en constante expansión, donde la inteligencia artificial generativa crea contenidos hiperrealistas, el análisis de datos se hace en lenguaje natural y las criptomonedas redefinen las transacciones económicas.

Pero ¿qué es la sobreexposición personal en la red?

Esta refiere al compartir excesiva información privada en línea de modo que pueda resultar incómoda o inaceptable y que tenga un impacto en la vida de las persona; ya sea porque al hacer pública dicha información pueda afectar la reputación del individuo ya sea en el trabajo u otros ámbitos, hasta incluso ser usada por ciberdelincuentes.

Si bien estas innovaciones han enriquecido nuestra vida, también han traído consigo nuevos desafíos y riesgos para la privacidad.

Más de una década después, el panorama ha cambiado

drásticamente. No solo nos encontramos ante una red ultra masificada, hiperconectada, sino que la aparición de tecnologías como la inteligencia artificial, el big data, y los algoritmos que gobiernan nuestras interacciones han exacerbado la complejidad de nuestra presencia digital.

Ya no se trata solo de lo que compartimos voluntariamente, sino también de cómo cada clic, cada "me gusta" y cada interacción es recopilada, analizada y usada para perfilar nuestra identidad digital.

De cómo cada sitio, cada aplicación y cada sistema manejan nuestros datos, como se interconectan con otros sistemas, como protegen esos datos y qué tan vulnerables son a intrusos.

La construcción del Yo Digital, que antes se limitaba a perfiles en redes sociales, la actividad en blogs y foros e historial de navegación, ahora se extiende a un universo de datos personales dispersos en múltiples plataformas.

Desde nuestros gustos musicales hasta nuestras ubicaciones en tiempo real, todo queda registrado y puede ser utilizado para fines comerciales, políticos e incluso malintencionados.

Ese Yo Digital, que describíamos como un reflejo de nuestra vida en el mundo físico, ha pasado a ser una

extensión ineludible de nosotros mismos. Se ha vuelto un espacio donde las fronteras entre lo público y lo privado están más borrosas que nunca, y donde la gestión de nuestra reputación, seguridad y privacidad ha dejado de ser opcional para convertirse en una necesidad.

En esta nueva edición iremos más allá del análisis inicial sobre la exposición personal en línea, buscando abordar los nuevos desafíos que surgen con la sobreexposición en la era de la hiperconectividad.

La creciente cantidad de dispositivos conectados, la integración de nuestras vidas a través de servicios de geolocalización, redes sociales basadas en intereses y la constante recolección de datos, nos obliga a preguntarnos: ¿dónde trazamos la línea entre lo privado y lo público? Y ¿cómo cuidamos no borrar con el codo esa línea que dibujamos con nuestra mano?

Haciendo un poco de memoria, al principio las redes sociales se identificaban según su tipo o propósito, con distintas implicaciones de privacidad y seguridad en su utilización.

Teníamos las redes personales que permiten a los usuarios crear perfiles detallados en línea y comunicarse con otros usuarios. Las redes de actualización de estado básicamente permiten a los usuarios publicar

actualizaciones generalmente cortas. Las redes de ubicación donde se registra actividades mediante el GPS del móvil. Las redes de intercambio de contenido están diseñadas como plataformas para compartir contenidos como música, fotografías y videos.

Incluso estas han evolucionado y comparten o combinan todos o casi todos estos propósitos en una misma red, dándole cada vez más datos, más acceso, más información.

Además hoy más que nunca, es crucial que comprendamos cómo interactuar de manera consciente con nuestro entorno digital. No se trata solo de protegernos de los riesgos, sino también de tomar decisiones informadas sobre cómo queremos ser percibidos y cómo gestionar nuestra identidad digital.

De poder desarrollar un pensamiento crítico que nos haga poder dudar de qué aplicación o sitio uso, qué comparto, con quién lo comparto y en dónde estoy compartiendo esta información.

Pero no solo para uno mismo, aquellos que somos padres debemos pensar en la privacidad de nuestros hijos, los riesgos específicos a los que están expuestos los niños y adolescentes en el mundo digital.

Los migrantes digitales tuvimos otro crecimiento, cuando éramos niños nuestros padres nos enseñaban de los peligros de cada cosa, a mirar para los dos lados antes de cruzar la calle porque era peligroso que estuviese circulando un vehículo y nos lastimara.

Sin embargo hoy con la tecnología esa enseñanza ha cambiado, tuvo un giro de 180°, muchas veces son los hijos quienes enseñan a sus padres como usar determinado producto o servicio digital, desconociendo los peligros que esto acarrea, evitando esa parte en la transferencia de conocimiento que se adquiere con la experiencia, que evidentemente no tienen y no han adquirido.

Este libro es una invitación a reflexionar sobre esos límites y a desarrollar capacidades prácticas que nos permitan navegar en esta realidad compleja de manera segura y responsable.

Adquirir herramientas y conocimientos necesarios para navegar de forma segura en un mundo cada vez más digital, proteger tus datos personales y tomar el control de tu identidad en línea.

Resumen del capítulo

Nuestra vida está constantemente expuesta en internet.

Todo aquello que compartimos queda registrado permanentemente, afectando nuestra privacidad y reputación.

Las nuevas tecnologías como inteligencia artificial, redes sociales y big data intensifican este fenómeno, creando nuevos desafíos sobre cómo proteger nuestra identidad digital y mantener el control sobre nuestros datos.

Identidad Social Online – El Yo Digital

En la actualidad, el concepto de identidad digital ha evolucionado considerablemente y cada vez más la identidad social en línea es un reflejo de nuestra personalidad en el mundo físico, una extensión de nosotros mismos.

Con las nuevas redes y tecnologías emergentes esta se ha vuelto más fragmentada, generando un grado mayor de dificultad para gestionarla.

Quizás por ello procedemos a interconectar perfiles propios, para actualizaciones centralizadas o simultaneas, dándole de esa forma a cada red o plataforma, acceso a información de los perfiles creados en las otras.

Lo que solía ser una manifestación más estática y manejada principalmente por las redes sociales tradicionales, hoy ha dado paso a un panorama mucho más complejo, marcado por algoritmos de inteligencia artificial, la IA generativa, el blockchain y por suerte una creciente conciencia sobre la privacidad y la seguridad en línea.

Actualmente, aplicaciones basadas en la inteligencia

artificial, como las herramientas de generación de contenido y asistentes virtuales, permiten automatizar aspectos de nuestra vida digital y de nuestras interacciones en este mundo.

Sin embargo, también agregan dificultad en la gestión de la información que se maneja en nuestra presencia en línea, ya que los algoritmos que personalizan la experiencia pueden recolectar y procesar datos sensibles sin que nos demos cuenta, o simplemente porque marcamos con un tic en “he leído y aceptado”.

La Identidad Digital tiene distintos enfoques ya sea filosófico o en psicológico, y al igual que al publicar SobreExposición Personal en la Red, la identidad sigue siendo un concepto multifacético que combina ambos aspectos.

Para la filosofía, la identidad es lo que define a una entidad y la distingue de otras. Mientras que en psicología la identidad de una persona se construye a partir de aspectos físicos y mentales únicos.

Sin embargo, en el mundo digital actual, estos conceptos están siendo redefinidos por la tecnología, donde ya no solo proyectamos una versión de nosotros mismos, sino múltiples versiones, varios "yo digitales", adaptados a distintos entornos virtuales.

¿Cuántos perfiles en aplicaciones o redes tienen una entidad física llamada persona? Muchos, distintos en propósito, comunicación, gestión y relacionamiento con terceras entidades.

Todos estos perfiles integran una identidad única, que nos define como individuos digitales, que refleja lo que somos, lo que pensamos, como nos relacionamos con las personas, con el mundo y con el conocimiento.

Incluso podemos llegar a decir que parte de nuestra mente está en la red, o mejor aún, que la red es parte integral de nuestro sistema cognitivo extendido.

La teoría de la mente extendida de Clarck y Chalmers se basa en el papel activo que el entorno tiene en la consecución de los procesos cognitivos, entorno con el que las interacciones se dan en ambas direcciones.

Estas interacciones crean un sistema ensamblado donde todos los componentes del mismo juegan un papel causal activo gobernando conjuntamente la conducta de un individuo.

Para afirmar esto los autores se basan en un Principio de Paridad que establece que, si al enfrentarnos a cierta tarea, algo externo a nosotros funciona como un proceso que si estuviese en la cabeza no dudaríamos en aceptarlo

como parte del proceso cognitivo, entonces ese algo, en ese momento, es parte de nuestro proceso cognitivo.

Este principio de paridad se sustenta en cuatro criterios que deben cumplirse para considerarse la cognición extendida.

I. El artefacto o el recurso que el agente posee tiene que ser confiable, estar disponible y ser normalmente invocado en la cognición.

II. La información recuperada debe ser automáticamente aceptada.

III. La información contenida en el artefacto o recurso tiene que ser fácilmente accesible cuando se la requiere.

IV. La información en el artefacto o recurso ha sido conscientemente aceptada en algún momento del pasado, y en efecto, hay una consecuencia de esta aceptación.

Para que sistemas acoplados sean relevantes en la cognición, se requiere que este sea considerado un acoplamiento confiable; si bien esto es más fiable dentro del cerebro, también puede haber un acoplamiento fiable con el entorno.

Si los recursos de mi celular, pc, calculadora o regla de carpintero están siempre ahí cuando los necesito, entonces estos estarán acoplados conmigo de la manera más confiable que necesitemos y serán parte del sistema cognitivo.

Otro ejemplo sencillo, básico y claro es la agenda de contactos que ubicamos en nuestro dispositivo móvil: hace poco tiempo esos registros estaban en nuestro cerebro o en una libreta junto al teléfono fijo en casa. Hoy ya casi no recordamos ningún número, usamos el móvil como almacenamiento y parte de nuestra memoria, con interacciones bidireccionales y un acoplamiento confiable.

O imagina que usamos el GPS en el teléfono para llegar a un lugar nuevo. Antes si necesitábamos encontrar una dirección, se usaban mapas de papel o indicaciones de otras personas. Hoy confiamos en el GPS para indicar el camino, considerándolo casi como una extensión de la capacidad para orientarte.

En ambos ejemplos la herramienta es confiable, siempre está disponible y la información es fácilmente accesible cuando la necesitas. Una herramienta externa se integra en tu proceso de pensamiento, funcionando como si fuera parte de tu propia mente.

De esta forma también podemos comprender que nuestra presencia en la red es una constante y la información que contiene sobre nosotros es relevante, sobre todo la compartida por uno mismo, nuestra identidad en línea pasa a ser parte de nuestra identidad física y se acoplan con fiabilidad.

Por lo que, así como decimos que nuestra identidad digital es el reflejo de nuestro ser en el mundo físico también esta interacciona en el otro sentido, accionando sobre nuestro ser en el mundo offline, incidiendo, influyendo en nuestra identidad fuera de línea y en el comportamiento, conformando una relación bidireccional.

Afectando lo que somos, quienes somos y nuestra relación con el mundo; conformando un único ser, un único sistema una nueva identidad combinada.

Hasta ahí parecería algo sencillo, pero esto no se queda allí, la identidad digital hoy tiene otra cara, la Personalización Algorítmica, la IA junto al Big Data nos acercan a una Identidad Proyectada.

Las grandes plataformas en línea, así como las pequeñas, todas aquellas que nos permiten crear perfiles de usuarios, registran cada interacción, manejan grandes volúmenes de datos e impulsadas por algoritmos de inteligencia artificial generan proyecciones basadas en

esos datos recogidos a lo largo del tiempo y del uso de estas por parte de las personas.

Es esa personalización algorítmica, la que por ejemplo nos muestra contenido adaptado a nuestros comportamientos pasados, recomendaciones basadas en inferencia por conductas anteriores, etc. la que influye en cómo nos percibimos y cómo otros nos ven.

Esta forma de identidad que conocemos como "identidad proyectada" se conforma desde el análisis de cada interacción que tenemos en plataformas como redes sociales, motores de búsqueda y tiendas en línea genera datos, nuestra huella digital, datos de diferentes clases, qué publicamos, qué buscamos, qué compramos y metadatos como cuánto tiempo dedicamos a un contenido, etc.

Su objetivo primario es anticiparse a las necesidades, gustos o comportamientos del usuario para personalizar recomendaciones, anuncios o servicios.

Utilizando tecnología para analizar esos patrones de comportamiento y construir perfiles únicos que alimentan la personalización algorítmica.

Si bien esto busca mejorar la experiencia del usuario al ofrecer recomendaciones relevantes, también influye en

nuestra percepción de la realidad. La identidad proyectada no solo refleja nuestras preferencias, sino que también las amplifica, reforzando creencias y comportamientos mediante la exposición constante a información alineada con ellas, pudiendo generar sesgos, burbujas de la realidad, de lo que vemos y consumimos.

Si bien todos los prestadores de servicios digitales trabajan para minimizarlas, estas burbujas de información son uno de los efectos negativos más evidentes de la hiperpersonalización. Los usuarios reciben contenido filtrado que coincide con sus intereses y creencias previas, pero rara vez se enfrentan a información que desafíe sus puntos de vista.

Este fenómeno, conocido como sesgo por perfilado, tiene imbuido el riesgo de poder llevar a las personas hacia una visión limitada del mundo, erosionando la diversidad de pensamiento y promoviendo la polarización.

Estas burbujas de información afectan la forma en que los demás nos perciben pudiendo amplificar prejuicios existentes en los datos, discriminando ciertos grupos basados en género, raza, edad, entre otros.

Desde un sitio de gestión financiera que puede profundizar inequidades, brechas sociales y económicas, recomendando o no, determinadas opciones o incluso

hasta tasas de financiamiento, tomando como datos de entrada nuestra identidad proyectada; hasta incluso filtrar qué oportunidades profesionales se nos presentan.

En este contexto, la gestión de nuestra información personal adquiere una relevancia crucial. Cada interacción en línea contribuye a la construcción de la identidad proyectada, lo que plantea interrogantes éticos y prácticos. ¿Qué tan conscientes somos de los datos que generamos? ¿Entendemos cómo se utilizan para influir en nuestras decisiones y percepciones?

Es necesario adoptar una postura proactiva hacia esa identidad digital que incluya varios aspectos como el controlar los datos compartidos; revisar configuraciones de privacidad y limitar la información que se comparte en cada plataforma, conocer cómo se almacena, con quién se comparte, que uso se le da.

Diversificar las fuentes de información; activamente buscar perspectivas distintas para evitar quedar atrapados en burbujas de información como forma de reentrenar al algoritmo constantemente.

Tener pensamiento crítico, cuestionar las recomendaciones algorítmicas, reflexionar sobre cómo y por qué se presenta cierto contenido, tratar de contraponerlo para evaluar su veracidad y completitud.

En este laberinto digital donde convergen múltiples 'yoes', la gestión consciente de nuestra identidad se vuelve imperativa.

No basta con ser meros espectadores de nuestra propia huella digital; debemos convertirnos en arquitectos activos de nuestra presencia en la red.

El futuro de nuestra identidad digital dependerá de nuestra capacidad para equilibrar la conveniencia de la hiperconectividad con la protección de nuestra privacidad.

Esto implica un ejercicio constante de autoconciencia, cuestionamiento crítico y adaptación a un entorno que se redefine a cada instante.

Solo así podremos navegar con seguridad y autenticidad en este vasto y complejo ecosistema digital, asegurando que nuestra identidad en línea sea un reflejo fiel de quienes somos, y no una simple proyección algorítmica.

Resumen del capítulo

Nuestra identidad digital ha evolucionado hacia múltiples versiones gestionadas por plataformas tecnológicas.

La personalización algorítmica genera identidades proyectadas que afectan nuestra vida offline.

Es crucial tomar conciencia y adoptar medidas para gestionar de forma segura nuestra presencia digital, evitar sesgos algorítmicos y proteger nuestra privacidad.

Evolución y Desafíos

Las redes sociales tradicionales, como Facebook, Instagram, X, continúan siendo lugares clave para la expresión de la identidad digital. Sin embargo, el anonimato y la privacidad, que alguna vez fueron un aspecto esencial de la red, ha sido erosionado casi por completo.

La combinación de reconocimiento facial, la vinculación entre plataformas y el rastreo de datos hacen que cada acción en línea sea rastreable con mayor celeridad y facilidad.

Muchas cosas han cambiado en estos años que afectan la privacidad y la seguridad de nuestra información personal.

Existe cada vez mayor cantidad de datos disponibles; estos datos personales que generamos y compartimos, ya sea intencionalmente o no, han aumentado exponencialmente. Las aplicaciones móviles, los dispositivos IoT y los asistentes virtuales, etc. recolectan una gran cantidad de información sobre nuestros hábitos, preferencias y ubicación.

La aparición de nuevas plataformas y funcionalidades a las ya existentes han ampliado las posibilidades de

compartir información personal. Por ejemplo, las historias de Instagram y los videos cortos de TikTok permiten compartir contenido efímero de manera rápida y sencilla, servicios o plataformas que hace 10 años no existían.

Incluso TikTok o BeReal han capitalizado la tendencia de la autenticidad instantánea, donde los usuarios comparten momentos de su vida en tiempo real, reduciendo aún más las barreras entre lo privado y lo público.

Pero también del otro lado de la balanza tenemos una mayor conciencia sobre la privacidad, a pesar del aumento de la sobreexposición, también ha crecido la conciencia sobre la importancia de la privacidad.

Muchas personas son más cuidadosas al compartir información personal y existen nuevas herramientas, internas de las plataformas o externas a estas, así como regulaciones nacionales o supra nacionales para proteger nuestros datos.

Y como es de esperarse con el desarrollo de la tecnología y el crecimiento de los datos aparecen nuevos riesgos asociados a estos, como las deepfakes, el doxing y hasta la manipulación de la información.

Estos cambios traen consigo una mayor dificultad para la

gestión de la identidad digital, la creciente cantidad de plataformas y la complejidad de las configuraciones de privacidad que estas presentan, junto con nuestra pereza para leer o entender los términos de uso por ejemplo, hacen que sea cada vez más difícil gestionar nuestra identidad digital de manera efectiva y saber realmente que compartimos y con quienes lo hacemos.

Ante esta situación surgen alternativas o formas de trabajar la identidad y los accesos a nuestros datos en estos sitios. Soluciones potenciadas por los avances de la tecnología y orientadas a cambiar el foco de poder, ya que para estas quién decide o permite el acceso a sus datos es el propio usuario.

Usando para ello Blockchain, esto no es solo Bitcoin, es una tecnología que consiste en un registro digital descentralizado y distribuido que almacena información en bloques conectados de manera cronológica y de forma segura mediante criptografía.

Al no depender de una autoridad central, la tecnología garantiza transparencia, seguridad y confianza, ya que las transacciones o cambios deben ser validados por una red de nodos, lo que dificulta el fraude o la manipulación de la información.

Esta tecnología ya es ampliamente utilizada en soluciones

varias donde la confianza y la verificación son esenciales y en nuestro caso se aplica a la “Descentralización de la Identidad”.

En contraposición a las identidades centralizadas que dependen de gobiernos, bancos, grandes corporaciones, aplicaciones o un sitio web; surge el concepto de identidad descentralizada o auto soberana mediante el uso de blockchain.

Esta tecnología permite a los usuarios controlar y verificar su identidad sin depender de intermediarios, descentralizando así la propiedad y la gestión de los datos. En este sistema, las identidades se almacenan en una blockchain, lo que garantiza seguridad, transparencia e inmutabilidad.

Cada usuario tiene una clave privada para gestionar y proteger su información personal, mientras que la blockchain actúa como un registro público que verifica la autenticidad de los datos sin necesidad de intermediarios.

¿Cómo sería esto? Imagina que tu identidad digital está en una libreta personal en la que anotas tus contactos y datos importantes. En lugar de guardar esta libreta en una sola oficina (como lo haría un banco o un gobierno), la libreta se guarda en varias copias repartidas entre amigos de confianza.

Cada vez que actualizas tu libreta, todos tus amigos se aseguran de que la información es correcta. Así, nadie puede modificarla sin que todos lo noten. Esto es, en esencia, lo que hace la tecnología blockchain: te da el control total de tu identidad sin depender de un solo intermediario.

Esto da la posibilidad a cada individuo de compartir solo la información necesaria con terceros, reduciendo el riesgos de fraude y protegiendo la privacidad.

Este es un enfoque clave para aquellos que promueven la creación de sistemas de identificación seguros, inclusivos y resistentes al control centralizado.

En un contexto donde la privacidad es cada vez más escasa, blockchain promete una solución diferente, que devuelve a las personas el control, total o parcial, sobre su información personal. Hecho este que se refleja en la iniciativa ID2020.

Es un punto crucial y que está cobrando cada vez más importancia. No hablamos de ONGs que buscan este tipo de soluciones, sino empresas como Microsoft con el Azure Decentralized Identity, sistemas como uPort, Sovrin.

La iniciativa ID2020, que busca y promueve el uso de blockchain para crear identidades digitales soberanas en

aplicaciones como servicios financieros, salud y ciudadanía global, es una alianza global que entre otras cosas busca crear sistemas de identidad digital inclusivos, seguros y respetuosos de la privacidad.

Fundada en 2016 buscando proporcionar identidades legales a las personas que carecen de ellas, especialmente en comunidades vulnerables y marginadas, sus bases promueven una identidad digital que mitigue riesgos como el robo de datos, la vigilancia masiva o el uso indebido de información personal.

La identidad descentralizada o auto soberana permite que los usuarios pueden compartir solo la información estrictamente necesaria para realizar una transacción o verificación, protegiendo otros datos en el camino.

Un usuario que utiliza un sistema con identidad digital respaldada por ID2020 podría, por ejemplo, demostrar su mayoría de edad para acceder a un servicio en línea sin necesidad de compartir su nombre, dirección o número de identificación. Esto protege su privacidad al evitar que datos sensibles queden expuestos o sean almacenados innecesariamente.

Ofrece herramientas que empoderan a los usuarios para gestionar sus identidades digitales de forma segura, ética y respetuosa con sus derechos.

Las interrogantes entonces hoy son, ¿Cuántos servicios en línea permiten usar este tipo de identidad para acceder a ellos? ¿Cuántas aplicaciones se irán sumando y lo permitirán en el futuro?

Nosotros como usuarios somos responsables también de exigir ese tipo de acceso a las plataformas de modo que este cambio se produzca con mayor celeridad.

Resumen del capítulo

La creciente complejidad tecnológica genera nuevos riesgos para la privacidad.

Plataformas emergentes y tecnologías como blockchain ofrecen soluciones para recuperar el control de nuestra identidad.

Entender estos avances y promover un uso responsable de los datos personales es esencial para protegernos frente a la sobreexposición.

Nuevos Riesgos a la Privacidad

Uno de los mayores desafíos al que nos enfrentamos hoy día es la manipulación de la identidad a través de tecnologías emergentes como las deepfakes.

Las deepfakes utilizan algoritmos de inteligencia artificial para crear videos o audios falsos extremadamente realistas que pueden dañar la reputación de una persona.

Generados sin su consentimiento, también son usados para fraguar estafas o engaños a terceros simulando ser una persona en particular.

Lamento informarte que estos algoritmos son entrenados con tus datos, tu propia información, audios, videos, fotos, etc., esos que vos compartís tan gentilmente con usuarios que no conoces realmente o con aplicaciones sin saber que concesiones estás aceptando.

Este nuevo fenómeno pone en riesgo no solo la privacidad, sino también la verdad misma en el entorno digital.

Estos videos o audios falsos, creados mediante algoritmos de aprendizaje profundo, son capaces de imitar de manera asombrosamente realista a cualquier persona, haciendo que sea cada vez más difícil distinguir entre lo real y lo falso.

La proliferación de los deepfakes representa un grave peligro ya que por un lado, ponen en riesgo la privacidad de las personas, ya que cualquier individuo puede convertirse en víctima de la creación de contenido falso que lo comprometa o difame.

Y por otro lado socavan la confianza en la información, ya que se utilizan para difundir noticias falsas, manipular la opinión pública y sembrar la desconfianza en las instituciones.

En un mundo cada vez más dependiente de la información digital, la capacidad de distinguir entre lo verdadero y lo falso se vuelve fundamental, y las deepfakes representan una amenaza a esta capacidad.

La lucha contra las deepfakes requiere un esfuerzo conjunto de gobiernos, empresas tecnológicas y sociedad en general.

Desarrollando nuevas herramientas y tecnologías para detectar y combatir la creación y difusión de este tipo de contenido falso, regulación de la inteligencia artificial o la creación de estándares para la autenticación de contenido digital son acciones necesarias, pero no suficientes.

Además, es fundamental la educación mediática; enseñar a las personas sobre los riesgos de estas deepfakes y

dotarlas de las herramientas necesarias para evaluar la veracidad de la información que encuentran en línea, contrastar fuentes, desarrollar un pensamiento crítico.

Solo a través de un enfoque multidisciplinario podremos protegernos de las amenazas que estas plantean en un mundo cada vez más complejo para preservar la integridad de nuestro entorno digital. Si bien representan un desafío sin precedentes, también son una oportunidad para desarrollar nuevas tecnologías y fortalecer nuestra capacidad crítica.

Pero las deepfakes no son todo el universo de problemas, ni siquiera son el problema que más frecuentemente afecta al público en general. Existen otros causados por nuestro propio comportamiento.

Según un estudio de Nature Human Behaviour se afirma que el 75% de los contenidos compartidos en redes sociales nunca fueron leídos por quienes los difundieron, simplemente ven un titular que confirma algún prejuicio y re compartieron sin leer.

Este comportamiento termina configurando un sesgo en la selección de contenidos digitales; los usuarios seleccionan y distribuyen aquello que confirme sus propias narrativas, lo que puede llevar a una distorsión de la realidad.

Las redes sociales han permitido difundir contenidos a gran escala, enlaces a noticias e información de asuntos públicos con sus respectivos hipervínculos que son de nuestro interés, o eso creemos, y decidimos compartirlos con otros.

Pero muchos usuarios lo hacen sin siquiera leer primero la información a la que estos enlaces apuntan. El estudio analiza más de 35 millones de publicaciones, del ámbito público de Facebook con localizadores uniformes de recursos compartidos entre 2017 y 2020 y llega a descubrir que el 75% de estos enlaces compartidos son "comparticiones sin clics" (SwoC por su sigla en inglés).

El contenido político extremo y alineado con el usuario recibió más SwoC, y aquellas personas con confirmaciones de prejuicios y sesgos tuvieron una participaron mayor que usuarios políticamente neutrales.

Los resultados sugieren que la viralidad del contenido político, ya sea información real o desinformación, está impulsada por un procesamiento superficial de titulares y anuncios en lugar del contenido central; lo que tiene implicaciones de diseño que permiten a inescrupulosos promover un discurso deliberado en la esfera pública en línea.

Hecho que facilita el trabajo y la consecución de

resultados para los creadores y difusores de fakenews o peor aún, para las deepfakes; en un mundo saturado de información.

Y no alcanza con una simple duda, la realidad exige desarrollar y aplicar el pensamiento crítico como enfoque para analizar, cuestionar y evaluar la información antes de aceptarla como verdadera, considerando las fuentes, el contexto y las intenciones detrás de los mensajes.

El pensamiento crítico nos hace desconfiar de lo superficial, ir más allá y buscar la evidencia detrás de las afirmaciones. Ante una información impactante, debemos verificar si proviene de medios confiables, si otras fuentes la corroboran y si está respaldada por datos verificables. Además debemos aprender a identificar sesgos, tanto en los textos como en nuestras propias percepciones.

Fomentar este tipo de razonamiento es una responsabilidad colectiva, desde la educación en escuelas hasta una responsabilidad individual en un uso consciente de las redes sociales. En última instancia, el pensamiento crítico no solo nos protege de contenido falso, sino que también fortalece nuestra capacidad de tomar decisiones basadas en hechos y no en desinformación.

Más allá de los riesgos tecnológicos evidentes, como las

deepfakes y la desinformación, existe una amenaza silenciosa pero igualmente peligrosa conocida como “ingeniería social”.

Esta se trata de un conjunto de técnicas utilizadas para manipular psicológicamente a las personas con el fin de obtener información confidencial o influir en su comportamiento.

A diferencia de los ataques cibernéticos tradicionales, que explotan vulnerabilidades en sistemas informáticos, la ingeniería social apunta directamente a la vulnerabilidad humana, aprovechándose de la confianza, el miedo, la curiosidad o la urgencia para inducir a las víctimas a actuar en contra de sus propios intereses.

Los delincuentes han perfeccionado sus métodos para engañar a las personas sin necesidad de recurrir a herramientas demasiado sofisticadas. En muchos casos, un simple correo electrónico o mensaje de texto que imita la identidad de una entidad legítima es suficiente para obtener credenciales, datos bancarios u otra información sensible.

En otros casos, los atacantes crean pretextos elaborados, como fingir ser empleados de soporte técnico o representantes de una institución confiable, persuadiendo a sus víctimas de revelar datos críticos, casi

todos tenemos algún conocido que ha sido víctima de este tipo de engaños para cosas tan triviales como robar tu cuenta de whatsapp.

También recurren a tácticas más sutiles, como la oferta de beneficios ficticios, sorteos, o la difusión de archivos infectados bajo la apariencia de contenido atractivo. Todo esto demuestra que en el fondo, la clave del éxito de la ingeniería social no radica en la tecnología, sino en la psicología humana.

Las redes sociales han facilitado enormemente la labor de estos delincuentes. Cada publicación, foto, comentario o reacción puede convertirse en una pieza del rompecabezas que permite a los atacantes perfilar a sus víctimas con gran precisión.

Analizando la información que compartimos públicamente, o aceptando conexiones de perfiles que no conocemos, pueden identificar patrones de comportamiento, predecir vulnerabilidades y crear engaños cada vez más personalizados.

Suplantar la identidad de un amigo o familiar para solicitar favores o información sensible es una táctica común, al igual que el uso de detalles personales para que un intento de fraude parezca más creíble.

Este fenómeno se ve amplificado por la SobreExposición (oversharing), que ya vimos es el compartir demasiada información en línea sin considerar las posibles consecuencias. Muchas personas no son conscientes del valor que tienen sus publicaciones y de cómo pueden ser utilizadas en su contra.

Damos información en perfiles públicos y aceptamos conexiones de perfiles que no conocemos, de gente que nunca vimos en redes privadas. Damos clic y aceptamos seguir y que nos sigan páginas, aplicaciones o pseudo empresas por un sorteo o promoción, sin verificar si son reales.

Dado que la ingeniería social se basa en la manipulación emocional y psicológica, la mejor defensa no es un software de seguridad, sino nuevamente la educación y la concientización.

Es fundamental desarrollar una mentalidad crítica y no confiar ciegamente en correos electrónicos, mensajes o llamadas inesperadas, especialmente cuando solicitan información personal o financiera.

Verificar la autenticidad de las fuentes antes de hacer clic en enlaces o descargar archivos, ya que una simple búsqueda puede ayudar a detectar fraudes.

También es importante ser cauteloso con la información que se comparte en redes sociales, ajustando las configuraciones de privacidad para limitar el acceso a los datos personales y manteniendo una red de contactos reales, conocidos y aceptados.

Otro aspecto clave en este tipo de engaños suele ser esa necesidad de urgencia de ciertas solicitudes. Los atacantes suelen crear un sentido de premura para evitar que la víctima piense con claridad, por lo que tomarse un momento para analizar la situación puede marcar la diferencia entre ser víctima de un engaño o evitarlo.

Además, la educación en ciberseguridad debe ser una prioridad tanto a nivel individual como colectivo, ya que compartir conocimientos con amigos, familiares y colegas contribuye a fortalecer una comunidad más protegida frente a estas amenazas.

Si bien las deepfakes y la desinformación representan un desafío creciente, la ingeniería social sigue siendo una de las formas más efectivas de ataque en el mundo digital.

No importa cuán avanzados sean los sistemas de seguridad; si un atacante logra convencer a una persona de que revele su contraseña, la tecnología poco podrá hacer para evitarlo.

La clave para combatir este tipo de amenazas radica en la educación y el desarrollo del pensamiento crítico.

Vivimos en un entorno donde la información es poder, y saber identificar intentos de manipulación y fraude es esencial para proteger nuestra privacidad y seguridad. En un mundo digital en constante evolución, la mejor defensa no es solo la tecnología, sino el conocimiento y la prevención.

Resumen del capítulo

La proliferación de deepfakes, ingeniería social y la difusión irresponsable de información generan amenazas crecientes para nuestra privacidad.

Combatir estas amenazas requiere educación, pensamiento crítico, regulación tecnológica y seguridad digital personal.

La Economía de la Reputación

En un mundo donde la información fluye en tiempo real, es analizada por algoritmos de inteligencia artificial, perfilada y procesada por estos, donde las interacciones digitales definen gran parte de nuestra identidad, la reputación en línea se ha convertido en un activo de incalculable valor.

Este intangible, que se construye a golpe de interacciones digitales, no solo impacta en nuestras relaciones personales y profesionales, sino que también tiene repercusiones económicas directas, influyendo en aspectos como la empleabilidad, el acceso a servicios financieros y la construcción de confianza en entornos comerciales.

La información personal, ese nuevo petróleo que alimenta la economía global, se ha convertido en el recurso más codiciado por empresas y gobiernos.

Cada interacción en la red, desde un comentario en redes sociales hasta una transacción en línea, es un dato que se mina, analiza y comercializa, conformando perfiles digitales que revelan nuestra identidad perfilada en profundidad.

Este valor intrínseco de los datos refleja cómo las empresas y organismos utilizan la información para dirigir campañas de marketing, influir en decisiones de consumo y, en ocasiones incluso, para buscar moldear la opinión pública.

Sin embargo, esta misma información, cuando cae en manos inescrupulosas o se gestiona de manera negligente, puede dañar irreparablemente nuestra reputación. Un dato filtrado, malinterpretado o utilizado maliciosamente puede desencadenar crisis de imagen, dañar relaciones profesionales e incluso alterar la percepción social de un individuo.

Por lo que la reputación en el mundo digital es un asunto tan delicado como crucial. En este contexto, la gestión de la reputación digital se revela como un tema tan delicado como trascendental. Proteger y administrar nuestra huella digital de manera proactiva se vuelve esencial.

La educación sobre privacidad, la transparencia en el uso de datos y la implementación de medidas de seguridad robustas no solo resguardan nuestra privacidad, sino que también fortalecen nuestra reputación en un entorno donde cada clic deja una cicatriz digital imborrable.

En definitiva, aprender a comprender y gestionar el valor de la información es un acto de empoderamiento que nos

permite navegar con confianza en un mundo donde los datos, en efecto, se han convertido en el nuevo petróleo.

Si bien hace años que se viene hablando de la importancia de la reputación en línea, hoy en día este tema ha adquirido una relevancia aún mayor, hasta el punto de que nuestra reputación debe gestionarse como la construcción de una marca personal.

Si miramos como afecta al mundo laboral, redes como LinkedIn han revolucionado la forma en que los profesionales construyen su identidad digital. En este ecosistema, la confianza se erige como la moneda de cambio, donde las conexiones, las recomendaciones y la actividad en la plataforma pueden abrir o cerrar puertas laborales.

La selección de personal ha trascendido de las entrevistas y currículums tradicionales. Los reclutadores y las empresas han adoptado herramientas de inteligencia artificial para analizar el comportamiento en redes sociales, las interacciones profesionales e incluso las opiniones expresadas en plataformas digitales.

Esto ha dado lugar a un nuevo paradigma, en el que algoritmos automáticamente diseñan nuestro perfil laboral, lo que hace que la gestión de esa marca personal se vuelva esencial para el crecimiento y la salud

profesional.

A medida que las redes sociales, las plataformas y hasta las aplicaciones que utilizamos avanzan en su capacidad de análisis, los algoritmos se vuelven más sofisticados.

Ya no solo rastrean nuestros intereses y movimientos, sino que también analizan patrones emocionales en nuestras interacciones, hábitos de consumo de contenido y transacciones digitales.

Si bien esto permite una personalización sin precedentes en la experiencia de usuario, también plantea interrogantes sobre la privacidad y la capacidad de los individuos para controlar su propia narrativa en línea.

El auge de la "cultura de la cancelación" es un claro ejemplo de cómo la reputación digital puede ser utilizada como un arma para imponer sanciones sociales y económicas. Comentarios antiguos, publicaciones desafortunadas o afiliaciones políticas pueden tener consecuencias duraderas en la carrera y en la vida personal de un individuo.

Para ser más claros, existen muchos casos de personas que han visto afectadas sus carreras o vidas personales por su actividad en línea.

El caso del director de cine James Gunn que fue

despedido por Disney en 2018 tras la reaparición de tuits antiguos con contenido de humor negro y temas controvertidos. Aunque fue recontratado meses después, el incidente dañó su reputación.

Pero no solo en Hollywood, varios Influencers y YouTubers creadores de contenido han perdido patrocinios y seguidores debido a comentarios o acciones inapropiadas en sus plataformas.

Hasta casos de "cancelación" a personas no famosas, ya sean profesores, estudiantes o empleados de diversas empresas han sido despedidos o sancionados por publicaciones en redes sociales que se consideraron ofensivas o inapropiadas.

Estos casos ilustran evidencian como una mala gestión de la reputación digital, el compartir cualquier cosa y sin pensar, puede tener un impacto duradero en la vida de las personas.

Puede terminar afectando oportunidades laborales, relaciones personales y percepción pública que tienen de nosotros.

La reputación digital está intrínsecamente ligada a la privacidad. La información que compartimos en línea, ya sea consciente o inconsciente, se utiliza para construir un

perfil sobre nosotros que puede ser utilizado de buena o mala manera, con buenas o malas intenciones.

Las empresas pueden utilizar esta información para segmentar publicidad o para evaluar nuestra solvencia crediticia, pero también puede ser utilizada por terceros malintencionados para suplantar nuestra identidad o para acosarnos.

La economía de la reputación también ha permeado en el sector financiero. Bancos y empresas fintech han incorporado algoritmos que analizan la información digital disponible para evaluar la solvencia de una persona.

Desde el historial de compras y la actividad en redes sociales, hasta la estabilidad de las relaciones profesionales pueden ser factores determinantes en el acceso al crédito.

Algunas de estas empresas han comenzado a utilizar "puntajes de confianza" basados en la actividad en línea, los cuales influyen en la capacidad de acceder a préstamos, alquileres e incluso determinados servicios.

Este modelo plantea dilemas éticos sobre la equidad y la discriminación algorítmica; ya que errores o sesgos algorítmicos en el procesamiento, análisis e

interpretación de los datos pueden afectar negativamente a individuos, grupos o minorías.

En la búsqueda de construir y mantener una reputación digital saludable, es fundamental ser transparentes y coherentes en nuestras interacciones en línea.

La autenticidad es valorada en el mundo digital, y tratar de proyectar una imagen falsa o pretenciosa puede ser contraproducente.

Es importante ser consciente de cómo nos presentamos y asegurarnos de que nuestra narrativa digital refleje los valores con que nos identificamos y nuestra identidad real.

Además, es esencial tener una actitud proactiva en el control de nuestra información personal y de nuestra reputación en línea. Esto implica revisar periódicamente nuestra actividad en redes sociales, eliminar contenido antiguo o irrelevante y asegurarnos de que nuestra información de perfil esté actualizada y sea precisa.

También es necesario estar al tanto de las políticas de privacidad de las plataformas que utilizamos y tomar medidas para proteger nuestra información personal. Evaluar cambios, leer antes de aceptar actualizaciones y analizar detenidamente las implicaciones de las nuevas

funcionalidades nos permitirá no quedar desprevenidos o en una posición de desventaja.

La velocidad y el alcance de las redes sociales pueden convertir un error o una publicación desafortunada en una crisis personal y profesional.

Por lo tanto debemos entender, aunque sea repetitivo, que es importante ser conscientes de la información que compartimos en línea y tomar medidas para proteger nuestra privacidad.

Resumen del capítulo

La reputación digital influye directamente en nuestra vida cotidiana, desde oportunidades laborales hasta acceso a servicios financieros.

La gestión consciente de esta reputación es fundamental, especialmente en una era donde cada interacción digital deja una huella imborrable.

Debemos ser proactivos, auténticos y cautelosos al compartir información en línea.

Permanencia y Memoria Colectiva

Hace más de una década hacíamos referencia a la idea de que "la red tiene memoria de elefante". Hoy esa metáfora no solo sigue siendo válida, sino que se ha intensificado en un entorno donde el volumen de información, la velocidad de difusión y las herramientas de análisis y búsqueda han alcanzado niveles nunca antes imaginados.

La capacidad para almacenar, indexar y recuperar datos ha evolucionado al punto de que, a pesar de los esfuerzos por borrar o disimular aspectos de nuestra vida personal, nuestro pasado digital se mantiene casi intacto.

Podríamos decir entonces que la Memoria Digital dispone de un almacenamiento infinito en la nube, si bien esto no es cierto, los recursos siempre son finitos, al fin de cuentas el crecimiento constante hace que así parezca.

La red cuenta con zettabytes de información donde cada publicación, comentario, fotografía o vídeo se añade a un vasto repositorio virtual, accesible a través de motores de búsqueda sofisticados como Google, Bing e incluso algoritmos especializados en redes sociales.

Incluso cuando intentamos borrar contenido comprometedor, el registro puede quedar almacenado en

cachés, archivos de sitios web o en bases de datos de terceros, lo que hace que la eliminación total sea prácticamente imposible.

La aparente inmediatez y la facilidad de acceso a esta información han modificado drásticamente la forma en que entendemos la privacidad y la construcción de nuestra identidad digital entorno a esta.

Todo esto ha traído aparejado un comportamiento de sobreexposición conocido como “extimidad”, esa necesidad de exteriorizar aspectos íntimos de nuestra vida, lo cual se ha intensificado con el auge de plataformas como Instagram, TikTok, Snapchat y LinkedIn.

Esta actitud que busca compartir detalles de la vida en línea, a veces con la esperanza de construir una imagen profesional o social atractiva, suele no acompañar del cuidado correcto ni medir las consecuencias de dejar una huella permanente.

Por lo cual la dicotomía entre la necesidad de privacidad y el impulso de la exposición se ha agudizado: por un lado, se busca el reconocimiento y la conexión inmediata, y por otro, se arriesga a perder el control sobre la narrativa personal.

Ejemplos recientes ilustran esta tensión. Un joven profesional puede ver cómo un vídeo viral en TikTok –quizá grabado en un momento de espontaneidad o descontrol– afecta sus oportunidades laborales, mientras que un comentario inofensivo hace años, rescatado por una búsqueda en línea, puede reaparecer en momentos críticos. Así, la exposición digital se convierte en una espada de doble filo, donde la construcción de la imagen y la reputación requieren cada vez más atención.

En la actualidad, la velocidad a la que se comparte la información es asombrosa. Lo que alguna vez se pensó como contenido "efímero" en plataformas como Snapchat o Instagram Stories, ahora es susceptible de ser capturado, reeditado y redistribuido en múltiples formatos y plataformas. La viralidad de un contenido, tanto positiva como negativa, puede transformar en cuestión de horas la percepción pública de una persona, afectando su reputación de manera duradera.

El fenómeno conocido como el "efecto Streisand" sigue vigente: los intentos de censurar o eliminar información pueden, irónicamente, aumentar su difusión. Este efecto se ha visto amplificado en un contexto donde los algoritmos no solo priorizan la novedad, sino también la controversia. Así, una simple solicitud de borrado puede acabar atrayendo la atención de miles de usuarios y hacer

que el contenido problemático se propague aún más.

Un ejemplo de esto es el caso de Elon Musk y el intento de bloquear el seguimiento de su jet privado. En diciembre de 2022, Musk suspendió la cuenta de Twitter "@ElonJet", que rastreaba los movimientos de su avión utilizando información pública.

Esto generó una ola de críticas y atención mediática, lo que resultó en una mayor difusión de la información que Musk intentaba ocultar.

Este caso muestra cómo el intento por ocultar información en la era digital puede tener el efecto contrario al deseado, especialmente cuando se trata de figuras públicas o temas de interés general.

La información, una vez publicada en internet, es difícil de eliminar por completo, y los intentos de hacerlo a menudo atraen más atención hacia ella.

Ante este panorama, han surgido industrias enteras dedicadas a la gestión de la reputación online. Empresas especializadas ofrecen servicios para “enterrar” resultados negativos en los buscadores, promoviendo contenidos positivos y ayudando a que la imagen digital de sus clientes sea más favorable. Sin embargo, estos servicios tienen límites y, a pesar de sus esfuerzos, es

imposible garantizar la eliminación completa de datos perjudiciales.

Paralelamente, en el ámbito normativo y regulatorio se han dado pasos importantes con legislaciones como el Reglamento General de Protección de Datos (GDPR) en Europa que ha introducido el “derecho al olvido”, permitiendo a los usuarios solicitar la eliminación de ciertos datos personales.

No obstante, esto no resulta algo simple para las distintas plataformas, la implementación de este derecho se enfrenta a desafíos técnicos y éticos; la dispersión de la información en múltiples servidores, la existencia de copias en dominios internacionales y la inherente dificultad de rastrear cada fragmento de datos en una red global. Así, pese a contar con herramientas legales para limitar el daño, la huella digital sigue siendo una realidad ineludible.

Y ahora tenemos la irrupción de la inteligencia artificial y el aprendizaje automático que han abierto nuevas posibilidades en el manejo y análisis de la información.

Como hemos mencionado las herramientas basadas en IA pueden reconstruir perfiles completos de individuos a partir de datos dispares, relacionando publicaciones, imágenes y comportamientos en línea para generar una

visión detallada –y a veces invasiva– de la vida personal de cada usuario.

Sumando a esto la tecnología de reconocimiento facial, combinada con bases de datos masivos, hace posible identificar a personas en fotografías y vídeos, aun cuando hayan sido publicados en contextos que se pretendían efímeros.

Y volvemos al punto de que esta capacidad de correlacionar datos plantea importantes dilemas éticos y de privacidad. Mientras la tecnología avanza, la brecha entre lo que se comparte de forma voluntaria y lo que es inferido a partir de patrones de datos se va reduciendo, haciendo que el control sobre la propia imagen digital sea cada vez más complejo. En este escenario, la conciencia sobre lo que se publica y el impacto a largo plazo se convierten en una necesidad imperante.

Frente a la permanente memoria de la red, nuevamente la educación y la responsabilidad personal se posicionan como herramientas clave. Campañas como "Piensa antes de publicar" han evolucionado para adaptarse a las nuevas dinámicas de interacción, invitando a los usuarios –especialmente a las generaciones más jóvenes– a reflexionar sobre las consecuencias de sus publicaciones para ellos y para terceros.

La conciencia de que cada acción digital puede tener repercusiones a nivel profesional, personal e incluso legal está transformando la forma en que se concibe la comunicación en línea.

Los nativos digitales, aquellos individuos que han crecido en un entorno hiperconectado, comienzan a mostrar actitudes más críticas respecto a su exposición en redes.

No obstante, la presión de ser visibles y relevantes en un mundo donde la imagen y la autenticidad parecen medirse en “likes” y comentarios sigue siendo poderosa.

Como en otros aspectos dela vida, la clave reside en encontrar un equilibrio: aprovechar las ventajas de la red para la autoexpresión y la conexión, sin perder de vista la necesidad de preservar una esfera privada y controlada.

La era digital actual ha llevado a la sobreexposición personal a niveles sin precedentes. La red, con su capacidad de almacenar y recuperar información de forma perpetua, nos obliga a repensar la relación entre privacidad y exposición.

Aunque existen herramientas y legislaciones para intentar mitigar el impacto de un pasado digital problemático, la realidad es que cada publicación puede ser recordada, reinterpretada y difundida en cualquier

momento.

En este contexto, el ejercicio de la discreción y la educación en el uso responsable de las tecnologías se convierten en elementos esenciales para gestionar nuestra identidad en línea.

La red tiene memoria, y en ella cada acción deja una huella. La pregunta que debemos hacernos es: ¿estamos dispuestos a asumir las consecuencias de nuestra presencia digital o preferiremos construir un entorno en el que la privacidad y la libertad de reinventarnos sean realmente posibles?

Resumen del capítulo

La información compartida en internet permanece casi indefinidamente, afectando la privacidad personal y profesional. Incluso intentos de eliminar contenidos pueden tener el efecto contrario.

La educación sobre los riesgos de compartir información y fomentar una cultura digital responsable son claves para protegernos ante este fenómeno permanente.

Una Identidad en Constante Evolución

La identidad digital ha dejado de ser una simple extensión de la identidad real para transformarse en un entramado complejo que incluye desde perfiles creados por cada individuo en distintos servicios digitales hasta proyecciones que se adaptan y son, en gran medida, reguladas por algoritmos y por las propias plataformas.

En esta era de convergencia entre lo físico y lo digital, la forma en que gestionamos y configuramos nuestro "yo digital" es vital para preservar no solo nuestra privacidad y reputación, sino también nuestra autonomía personal.

A lo largo de los últimos años, la transformación digital ha reconfigurado la manera en que nos relacionamos con la información y cómo nos presentamos en el entorno virtual.

Cada interacción en línea, ya sea una publicación en redes sociales, una transacción financiera o una búsqueda en internet, deja una huella que, acumulada, conforma un perfil complejo y multifacético.

Esta exposición, a menudo inconsciente, abre la puerta a riesgos como el robo de identidad, el ciberacoso y la manipulación de nuestra imagen en la red, aspectos que

han cobrado una relevancia sin precedentes en la sociedad contemporánea.

Para contrarrestar estos desafíos, resulta indispensable adoptar estrategias que vayan más allá del uso básico de herramientas tecnológicas. La encriptación de datos, la autenticación de dos factores y el empleo de software de ciberseguridad son recursos esenciales, pero su eficacia se potencia cuando se acompañan de una sólida cultura de alfabetización digital.

Conocer las tácticas de phishing, identificar intentos de malware o comprender la magnitud de la vigilancia masiva son conocimientos que empoderan al usuario y lo convierten en el primer eslabón de la cadena de defensa contra las amenazas digitales.

La educación digital también es fundamental para proveer a los individuos de herramientas que le ayuden en el manejo de su información personal.

Es necesario fomentar una conciencia crítica acerca de qué datos compartir, en qué contextos y con quién la compartimos, comprendiendo que cada publicación configura la huella digital, y que esta puede perdurar en el tiempo.

Al integrar programas de formación en ciudadanía digital

se promueve un uso responsable de las redes, evitando la sobreexposición y fortaleciendo la protección de la privacidad.

Este enfoque educativo no solo reduce los riesgos asociados a la difusión indiscriminada de información propia o de terceros, sino que también impulsa una cultura de cautela y autorreflexión que contribuye a una identidad digital más segura y consciente.

La integración creciente de la inteligencia artificial en la gestión de contenidos y la toma de decisiones añade otra capa de complejidad a nuestro entorno digital. Los algoritmos no solo filtran y organizan la información, sino que también pueden moldear nuestras percepciones y comportamientos.

En este contexto, resulta crucial cuánto los usuarios como los desarrolladores y legisladores colaboren en la creación de marcos regulatorios que garanticen la transparencia y el respeto por los derechos individuales.

La responsabilidad de proteger la identidad digital no recae únicamente en las empresas tecnológicas, sino que es un compromiso colectivo que involucra a toda la sociedad.

En este entorno interconectado resulta indispensable que

el proceso regulatorio sea colaborativo y adaptativo. Es fundamental que instituciones gubernamentales, empresas tecnológicas, organizaciones de la sociedad civil y expertos en ética trabajen en conjunto para diseñar normativas flexibles, capaces de evolucionar al ritmo de las innovaciones digitales.

Este enfoque cooperativo debe buscar un equilibrio entre el fomento de la innovación y la protección de los derechos fundamentales, garantizando que las nuevas tecnologías se implementen de manera responsable y transparente.

Asimismo, se requiere un compromiso activo de todas las plataformas y aplicaciones, para fomentar la rendición de cuentas en el uso de algoritmos y en la gestión de la información personal que estas almacenan y procesan en pos de la transparencia.

Implementar mecanismos de auditoría independientes y políticas de control que permitan detectar y corregir cualquier desviación en el manejo de datos, garantizando que las prácticas sean éticas y respetuosas con los derechos individuales.

Todos estos actores deben participar en un diálogo constante que facilite la supervisión de prácticas digitales y la creación de mecanismos de control conjuntos.

Solo a través de un enfoque integral y colaborativo se podrá construir un ecosistema digital en el que la protección de la identidad y la privacidad de los individuos sea una prioridad compartida.

Paralelamente, la expansión del Internet de las Cosas (IoT) ha multiplicado los puntos de contacto a través de los cuales se genera y comparte información.

Desde dispositivos inteligentes en nuestros hogares hasta wearables y sistemas integrados en vehículos, cada objeto conectado se suma a la compleja red que constituye nuestra identidad digital.

Esta interconexión demanda una gestión ética y responsable, en la que la privacidad y la seguridad se conviertan en valores innegociables a lo largo de todo el ecosistema digital.

La regulación debe evolucionar para asegurar que el manejo de la información respete tanto la autonomía individual como la diversidad cultural y social.

Otro aspecto fundamental en la dimensión ética es la gobernanza de los datos. En un mundo donde el “big data” permite el análisis a gran escala de comportamientos y preferencias, se hace imprescindible establecer límites claros que protejan la integridad de la persona.

El uso de estas herramientas para la interconexión de bases de datos, incluso aquellas de menor escala, se ha convertido en una herramienta poderosa para perfilar identidades.

Los sistemas que cruzan y analizan registros personales, aparentemente inofensivos de forma individual, pueden combinarlos para revelar patrones, comportamientos y conexiones que permiten una visión sorprendentemente detallada del individuo.

Este proceso de agregación de datos, si bien facilita la personalización y optimización de servicios, también representa un riesgo importante, ya que la fusión de diversas fuentes incrementa la vulnerabilidad de la información personal y contribuye a la erosión de la privacidad.

El manejo y la compartición de estos datos por parte de aplicaciones y sistemas sin un control riguroso pueden desembocar en escenarios de explotación indebida.

Es fundamental implementar protocolos de seguridad y marcos regulatorios robustos que limiten el acceso y la transferencia de información sensible.

Solo mediante una gobernanza ética y colaborativa se podrá garantizar que el análisis y la interconexión de

bases de datos se realicen de manera transparente, protegiendo así la integridad y el derecho a la privacidad de cada individuo.

En definitiva, el futuro del "yo digital" depende de nuestra capacidad para adaptarnos a un entorno en constante cambio y para trazar, de forma consciente, la línea entre lo público y lo privado.

Proteger nuestra información personal y gestionar con responsabilidad nuestra reputación en línea no es solo una necesidad técnica, sino también un compromiso ético y social.

En la medida en que la tecnología continúe evolucionando, también lo deberán hacer nuestras estrategias de defensa y control, haciendo que la construcción y mantenimiento de una identidad digital robusta sea, sin duda, uno de los desafíos más importantes de la era contemporánea.

Resumen del capítulo

La evolución constante del entorno digital demanda estrategias adaptativas para proteger nuestra identidad.

La integración de tecnologías como la IA y el IoT requiere marcos regulatorios claros y educación digital continua para garantizar privacidad y seguridad en un entorno que cambia continuamente.

Recomendaciones y medidas prácticas

Ya hemos resaltado que en esta era digital, donde la sobreexposición y las amenazas a la privacidad son una preocupación constante, es fundamental tomar medidas proactivas para proteger nuestra información personal y nuestra seguridad en línea.

Para esto el papel de la educación y la alfabetización digital es fundamental en la prevención de la sobreexposición, manifestada de diversas formas, desde la saturación de información y estímulos digitales hasta la exposición excesiva a contenidos perjudiciales o la dependencia tecnológica.

En este contexto, la formación en ciudadanía digital es la principal herramienta para lograr navegar de manera segura, crítica y equilibrada en el entorno digital, minimizando los riesgos asociados.

Recordemos que los usuarios de la red son heterogéneos, compuesta por todo tipo de personas, de edades muy dispares, desde nativos digitales a baby boomers, de personas con baja educación formal a otras con educación avanzada.

El enfoque, la preparación y la capacitación por

consiguiente no es única, ni general a todos los individuos y esta deberá ser multidisciplinaria.

La educación debe proporcionar una base sólida para el desarrollo del pensamiento crítico y para el consumo de medios, de forma de poder analizar fuentes, identificar sesgos, contrastar datos y formar juicios informados.

Recordemos que este pensamiento crítico actúa como un filtro protector contra la exposición a noticias falsas, contenido manipulador o propaganda, permitiendo a los individuos tomar decisiones más conscientes sobre lo que consumen, a lo que se exponen y lo que re comparten.

Pero las competencias digitales van más allá de esto; deben dotar a las personas con las habilidades específicas necesarias para desenvolverse eficazmente en el entorno digital.

Esto incluye la comprensión de cómo funcionan las distintas tecnologías, el desarrollo de habilidades para buscar, evaluar y utilizar información digital de manera eficiente, la conciencia sobre los riesgos y oportunidades en línea, así como la capacidad de comunicarse y colaborar digitalmente de forma segura y responsable.

También debe abarcar la comprensión de conceptos como la privacidad en línea, la seguridad cibernética y la huella

digital.

Todos estos elementos son cruciales para protegerse de la sobreexposición y de riesgos como el ciberacoso, el robo de identidad o la manipulación algorítmica.

Al entender cómo funcionan las plataformas digitales y cómo gestionan nuestra información, las personas pueden tomar medidas proactivas para limitar su exposición a contenidos no deseados o perjudiciales y proteger su bienestar digital.

A través de la educación, se promueve la conciencia sobre los propios hábitos digitales, la reflexión sobre el impacto del uso de la tecnología en la vida personal y la adquisición de estrategias para establecer límites saludables en el consumo digital.

Si bien la tecnología y las plataformas evolucionan constantemente, existen principios y prácticas fundamentales que podemos aplicar para reducir riesgos y navegar por el mundo digital de manera más segura, genéricas de modo que sean de utilidad con el paso del tiempo.

Lo primero que podemos hacer es tomar conciencia sobre la gestión de la privacidad en redes sociales.

Para ello debemos realizar una configuración detallada de

cada plataforma, servicio o red que usemos. Revisar y ajustar la configuración de privacidad de cada red social que utilices.

Recorrer, leer y familiarízate con las opciones disponibles y personalízalas según tus preferencias y el tipo de información que desees compartir o no compartir.

Otra opción es crear listas y grupos para segmentar a tus contactos y controlar quién tiene acceso a tus publicaciones, a quién le das acceso a cada cosa que compartes en la red.

Compartir información personal solo con personas de confianza es fundamental, controlar a quién aceptamos como contacto, donde, que cosas publicamos y que información le damos a los contactos. ¿Conocemos esa persona o empresa en el mundo real? Es una pregunta importante antes de aceptar una conexión.

Tener precaución al compartir, evita publicar información personal sensible como tu dirección, número de teléfono, datos bancarios o detalles de tus planes. Debemos reflexiona sobre el impacto que puede tener la información que compartes, piensa antes de compartir.

Una revisión periódica de tu actividad en redes sociales, post antiguos, es importante para cuidar la reputación

digital, y eliminar contenido antiguo o irrelevante que ya no deseas compartir o que sea público.

La red nunca olvida pero es necesario revisar de tanto en tanto la memoria colectiva dado que nuestras opiniones o ideas pueden variar con el tiempo.

Luego tenemos que pensar en la seguridad en los dispositivos que utilizamos para acceder a la red.

Utilizar contraseñas únicas y complejas para cada una de tus cuentas. Combina letras mayúsculas y minúsculas, números y símbolos. Actualmente incluso ya hablamos de frases como contraseña.

Actualmente incluso ya hablamos de frases como contraseña.

Tener una gestión segura de estas, no reutilices contraseñas en diferentes servicios.

Podemos utilizar un gestor de contraseñas para generar y almacenar contraseñas complejas de forma segura y no perder el control de las mismas o caer en la tentación de usar siempre la misma y no cambiarla jamás.

Habilitar autenticación de dos factores (2FA) siempre que sea posible.

Esta medida de seguridad adicional requiere un segundo

factor de verificación (como un código enviado a tu teléfono) para acceder a tu cuenta, lo que dificulta el acceso no autorizado.

Mantén tus dispositivos (ordenador, móvil, tablet, etc.) actualizados con las últimas versiones de software y parches de seguridad.

Las actualizaciones suelen incluir mejoras de seguridad importantes y las vulnerabilidades del software desactualizado es el que los piratas informáticos suelen aprovechar para acceder a estos.

Tener instalado un software antivirus y antimalware confiable y mantenlo actualizado.

Pero solo tenerlo no es suficiente, es necesario realizar análisis periódicos de tus dispositivos para detectar y eliminar posibles amenazas.

Un problema común son las redes wifi públicas, evita conectarte a redes wifi públicas no seguras, ya que pueden ser utilizadas para interceptar tus datos.

Si necesitas utilizar una red wifi pública, considera utilizar una red privada virtual (VPN) para proteger tu conexión o hacer un uso puntual de las mismas, y siempre contar con software antivirus y anti-malware actualizado.

Y finalmente el comportamiento en línea es un punto especial. Pensar antes de publicar, reflexionar sobre el contenido que vas a publicar y el impacto que puede tener en ti y en otros.

Una vez publicado, el contenido puede ser difícil de eliminar por completo.

Comparte solo la información necesaria y evita revelar detalles innecesarios sobre tu vida personal, la sobreexposición es un problema real, constante y no dimensionado correctamente por las personas.

Siempre tener una postura de pensamiento crítico, desconfiar de ofertas, publicidad y sorteos sospechosos, especialmente aquellos que solicitan información personal o financiera.

Siempre verificar la información que encuentras en línea antes de re compartirla.

Contrasta fuentes confiables y evita propagar noticias falsas o desinformación, leer lo que vamos a compartir y compartir contenido sin clics (SwoC).

Existen en la red herramientas y recursos que pueden ser de utilidad y ayudarnos a navegar en forma más segura.

Utilizar software de privacidad y seguridad confiable,

como antivirus, antimalware, VPN y extensiones de navegador para proteger tu privacidad.

Familiarizarnos con plataformas de verificación de noticias y herramientas de detección de deepfakes para evaluar la veracidad de la información que encuentras en línea.

Consultar organizaciones y recursos en línea especializados en privacidad y seguridad para mantenerte informado sobre las últimas amenazas y aprender nuevas estrategias de protección.

Al seguir estas recomendaciones y adoptar un enfoque proactivo hacia tu privacidad y seguridad en línea, podrás navegar por el mundo digital con mayor confianza y proteger tu identidad de manera efectiva.

Reiterativo hasta el cansancio, la principal herramienta es la educación y la alfabetización digital. Estas no son solo habilidades técnicas, sino herramientas fundamentales para la prevención de la sobreexposición en la era digital.

Al fomentar el pensamiento crítico, la conciencia digital, las habilidades de autorregulación y el comportamiento en línea responsable, las personas pueden navegar por el mundo digital de manera segura, informada y

equilibrada, minimizando los riesgos de la sobreexposición y promoviendo un uso saludable y productivo de la tecnología.

Resumen del capítulo

Proteger nuestra privacidad requiere acciones concretas como ajustar configuraciones de seguridad, utilizar autenticación multifactor, mantener actualizados nuestros dispositivos y practicar un pensamiento crítico ante la información digital.

La educación y alfabetización digital continua son herramientas imprescindibles para enfrentar la sobreexposición y riesgos asociados.

Recursos útiles para proteger tu privacidad y seguridad en línea

Estas recomendaciones, ya sean sitios web, aplicaciones o agregados para los navegadores, no constituyen una lista exhaustiva, existen muchos más recursos que nos ayudarán en esta actividad de forma de asegurar nuestra seguridad y privacidad.

La siguiente es una lista que sin ser completa trata de abarcar todos los aspectos posibles.

Organizaciones y sitios web:

- INCIBE (Instituto Nacional de Ciberseguridad - España): https://www.incibe.es/
- OSI (Oficina de Seguridad del Internauta - España): https://www.incibe.es/ciudadania
- Agencia Española de Protección de Datos: https://www.aepd.es/
- CNIL (Commission Nationale de l'Informatique et des Libertés - Francia): https://www.cnil.fr/fr
- ICO (Information Commissioner's Office - Reino Unido): https://ico.org.uk/
- NIST (National Institute of Standards and

Technology - Estados Unidos):
https://www.nist.gov/

- Electronic Frontier Foundation (EEUU):
https://www.eff.org/
- Access Now (Internacional):
https://www.accessnow.org/
- Derechos Digitales (Latinoamérica):
https://www.derechosdigitales.org/

Herramientas y extensiones de navegador:

- Gestores de contraseñas: 1Password, LastPass, Bitwarden
- Extensiones de privacidad: uBlock Origin, Privacy Badger, HTTPS Everywhere
- Buscadores privados: DuckDuckGo, Startpage
- Redes privadas virtuales (VPN): ProtonVPN, NordVPN, ExpressVPN

Plataformas de verificación de noticias:

- Newtral.es (España): https://www.lasexta.com/temas/newtrales-1
- Snopes (Estados Unidos): https://www.snopes.com/fact-check/
- PolitiFact (Estados Unidos): https://www.politifact.com/
- Chequeado (Latinoamérica): https://chequeado.com/
- FactCheck.org (Estados Unidos): https://www.factcheck.org/

Glosario

Algoritmo: Conjunto de reglas e instrucciones sistemáticas que se utilizan para resolver un problema o realizar una tarea específica, especialmente en el ámbito de la informática.

Autenticación de dos factores (2FA): Es una capa adicional de seguridad que usa dos formas de verificación para acceder a tu cuenta. Primero algo conocido como tu contraseña y segundo algo que tienes, como un código de verificación enviado a tu teléfono o una aplicación de autenticación.

Big Data: Se refiere a conjuntos de datos masivos y complejos que superan la capacidad de las herramientas de procesamiento de datos tradicionales.

Blockchain: Tecnología que permite la creación de registros digitales seguros y descentralizados de transacciones o información.

Ciberacoso: Uso de medios digitales para acosar, intimidar o humillar a una persona.

Contenido compartido sin clic (SwoC): Es cuando los usuarios comparten un enlace o contenido en redes

sociales sin haber hecho clic en él mismo. Esto puede ocurrir por confiar en el título, la fuente o simplemente para generar conversación, sin verificar el contenido completo.

Deepfake: Técnica que utiliza inteligencia artificial para crear videos o audios falsos pero realistas, a menudo con el objetivo de difamar o engañar.

Doxing: Revelación pública de información privada o identificativa de una persona en Internet, generalmente con malas intenciones.

Huella Digital: El rastro de datos que dejamos al navegar por Internet y utilizar servicios en línea.

Identidad Digital: Representación en línea de una persona, que puede incluir información personal, perfiles en redes sociales, etc.

Identidad proyectada: Representación de una persona, realizada por distintas plataformas, filtrada y adaptada por algoritmos de IA.

Ingeniería Social: Práctica de manipular psicológicamente a las personas para obtener información confidencial o lograr que hagan algo en contra de sus intereses.

Internet de las Cosas (IoT): La interconexión de objetos cotidianos a Internet, permitiéndoles recopilar e intercambiar datos.

Metaverso: Entornos virtuales inmersivos donde los usuarios pueden interactuar entre sí y con elementos digitales.

Personalización Algorítmica: Adaptación de contenido o servicios en línea basada en el análisis de datos y el uso de algoritmos.

Phishing: Intento de obtener información confidencial (como contraseñas o datos bancarios) mediante el engaño, a menudo a través de correos electrónicos o sitios web falsos.

Privacidad: Derecho a controlar la información personal y a decidir quién tiene acceso a ella.

Reputación en Línea: Percepción que tienen otros sobre una persona o entidad en el entorno digital.

Sesgo por Perfilado: Ocurre cuando los algoritmos de personalización refuerzan los prejuicios existentes en los datos, limitando la diversidad de información que se muestra a los usuarios.

Sobreexposición: Exceso de información personal compartida en línea, lo que puede generar riesgos para la privacidad y la seguridad.

Yo digital: La imagen que una persona proyecta en Internet a través de sus interacciones y comportamientos.


ISBN: 978-9915-43-151-2
9 789915 431512